CLAIMS

1. A method of obtaining a resource from a resource provider (RP) for a resource requester (RR) operating on a computing device, the RR having an identity descriptor (id) associated therewith, the id including security-related information specifying an environment in which the RR operates, the method comprising:

loading the RR onto the computing device;

loading the id corresponding to the RR onto the computing device;

providing the RR with a reference to the loaded id;

calculating a code identity (code-ID) corresponding to and based on the loaded RR and loaded id;

receiving a request from the RR for the resource;

ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource;

forwarding the request for the resource from the RR to the RP, the forwarded request including the calculated code-ID for the requesting RR, the id for the requesting RR, and a definition of the resource requested by the RR, the RP verifying that the calculated code-ID in the forwarded request matches one of one or more valid code-IDs for the identified RR, concluding based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy, and responding to the forwarded request by providing the requested resource;

receiving, by the RR, the requested resource as provided by the RP, and employing same in a manner consistent with the trust imparted to the

RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

2. The method of claim 1 comprising an authenticator on the computing device ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource wherein, the authenticator referring to the security-related information in the id corresponding to the RR.

3. The method of claim 1 wherein the forwarded request further includes a digital signature based on at least one of the calculated code-ID for the requesting RR, the id for the requesting RR, and the definition of the resource requested by the RR, the signature being verifiable based on a security key shared with the RP.

4. The method of claim 1 wherein the id includes therein a set of security-related name-value pairs available as input to at least one of the RR, the RP, and an operating system on the computing device upon which the RR operates.

5. The method of claim 4 wherein the name-value pairs describe at least one of the environment within which the RR operates, whether the RR is to be operated in an isolated process, and each entry point by which the RR can be accessed.

6. The method of claim 1 wherein the code-ID is calculated from a digest of the RR and the id.

7. The method of claim 6 wherein the code-ID is a hash of the RR concatenated with the id thereof.

8. The method of claim 7 wherein the code-ID is a concatenation of two hashes, each hash being of the RR concatenated with the id thereof.

9. A method of providing a resource by a resource provider (RP) to a resource requester (RR) operating on a computing device, the RR having an identity descriptor (id) associated therewith, the id including security-related information specifying an environment in which the RR operates, the method comprising:

receiving a forwarded request from the RR for the resource, the forwarded request including a code identity (code-ID) calculated for the requesting RR, the calculated code-ID corresponding to and based on the RR and the id as loaded on the computing device, the forwarded request also including the id for the requesting RR and a definition of the resource requested by the RR;

verifying the received request;

obtaining the code-ID, the id, and the definition of the resource requested from the received request;

determining from the received request an identity of the requesting RR;

obtaining each of one or more valid code-IDs for the identified RR;

verifying that the calculated code-ID in the received request matches one of one or more valid code-IDs for the identified RR and concluding based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy;

responding to the forwarded request by providing the requested resource to the RR, the RR receiving the requested resource as provided by the RP and employing same in a manner consistent with the trust imparted to the RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

10. The method of claim 9 comprising receiving the forwarded request from an authenticator on the computing device ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource wherein, the authenticator referring to the security-related information in the id corresponding to the RR.

11. The method of claim 9 wherein the forwarded request further includes a digital signature based on at least one of the calculated code-ID for the requesting RR, the id for the requesting RR, and the definition of the resource requested by the RR, the method further comprising verifying the signature.

12. The method of claim 9 further comprising validating the forwarded request based on other information therein.

13. The method of claim 9 further comprising determining that the requested resource is available and/or can be provided.

14. The method of claim 9 wherein the id includes therein a set of security-related name-value pairs available as input to at least one of the RR, the RP, and an operating system on the computing device upon which the RR operates.

15. The method of claim 14 wherein the name-value pairs describe at least one of the environment within which the RR operates, whether the RR is to be operated in an isolated process, and each entry point by which the RR can be accessed.

16. The method of claim 9 wherein the code-ID is calculated from a digest of the RR and the id.

17. The method of claim 16 wherein the code-ID is a hash of the RR concatenated with the id thereof.

18. The method of claim 17 wherein the code-ID is a concatenation of two hashes, each hash being of the RR concatenated with the id thereof.

19. A computer-readable medium having stored thereon computer-executable instructions for performing a method of obtaining a resource from a resource provider (RP) for a resource requester (RR) operating on a computing device, the RR having an identity descriptor (id) associated therewith, the id including security-related information specifying an environment in which the RR operates, the method comprising:

loading the RR onto the computing device;

loading the id corresponding to the RR onto the computing device;

providing the RR with a reference to the loaded id;

calculating a code identity (code-ID) corresponding to and based on the loaded RR and loaded id;

receiving a request from the RR for the resource;

ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource;

forwarding the request for the resource from the RR to the RP, the forwarded request including the calculated code-ID for the requesting RR, the id for the requesting RR, and a definition of the resource requested by the RR, the RP verifying that the calculated code-ID in the forwarded request matches one of one or more valid code-IDs for the identified RR, concluding based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be

trustworthy, and responding to the forwarded request by providing the requested resource;

receiving, by the RR, the requested resource as provided by the RP, and employing same in a manner consistent with the trust imparted to the RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

20. The medium of claim 19 wherein the method comprises an authenticator on the computing device ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource wherein, the authenticator referring to the security-related information in the id corresponding to the RR.

21. The medium of claim 19 wherein the forwarded request further includes a digital signature based on at least one of the calculated code-ID for the requesting RR, the id for the requesting RR, and the definition of the resource requested by the RR, the signature being verifiable based on a security key shared with the RP.

22. The medium of claim 19 wherein the id includes therein a set of security-related name-value pairs available as input to at least one of the RR, the RP, and an operating system on the computing device upon which the RR operates.

23. The medium of claim 22 wherein the name-value pairs describe at least one of the environment within which the RR operates, whether the RR is to be operated in an isolated process, and each entry point by which the RR can be accessed.

24. The medium of claim 19 wherein the code-ID is calculated from a digest of the RR and the id.

25. The medium of claim 24 wherein the code-ID is a hash of the RR concatenated with the id thereof.

26. The medium of claim 25 wherein the code-ID is a concatenation of two hashes, each hash being of the RR concatenated with the id thereof.

27. A computer-readable medium having stored thereon computer-executable instructions for performing a method of providing a resource by a resource provider (RP) to a resource requester (RR) operating on a computing device, the RR having an identity descriptor (id) associated therewith, the id including security-related information specifying an environment in which the RR operates, the method comprising:

receiving a forwarded request from the RR for the resource, the forwarded request including a code identity (code-ID) calculated for the requesting RR, the calculated code-ID corresponding to and based on the RR and the id as loaded on the computing device, the forwarded request also including the id for the requesting RR and a definition of the resource requested by the RR;

verifying the received request;

obtaining the code-ID, the id, and the definition of the resource requested from the received request;

determining from the received request an identity of the requesting RR;

obtaining each of one or more valid code-IDs for the identified RR;

verifying that the calculated code-ID in the received request matches one of one or more valid code-IDs for the identified RR and concluding based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon

which the RR operates is known security-related information that can be presumed to be trustworthy;

responding to the forwarded request by providing the requested resource to the RR, the RR receiving the requested resource as provided by the RP and employing same in a manner consistent with the trust imparted to the RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

28. The medium of claim 27 wherein the method comprises receiving the forwarded request from an authenticator on the computing device ascertaining that the requesting RR has rights to the resource and is to be trusted with the resource wherein, the authenticator referring to the security-related information in the id corresponding to the RR.

29. The medium of claim 27 wherein the forwarded request further includes a digital signature based on at least one of the calculated code-ID for the requesting RR, the id for the requesting RR, and the definition of the resource requested by the RR, the method further comprising verifying the signature.

30. The medium of claim 27 wherein the method further comprises validating the forwarded request based on other information therein.

31. The medium of claim 27 wherein the method further comprises determining that the requested resource is available and/or can be provided.

32. The medium of claim 27 wherein the id includes therein a set of security-related name-value pairs available as input to at least one of the RR, the RP, and an operating system on the computing device upon which the RR operates.

33. The medium of claim 32 wherein the name-value pairs describe at least one of the environment within which the RR operates, whether the RR is to be operated in an isolated process, and each entry point by which the RR can be accessed.

34. The medium of claim 27 wherein the code-ID is calculated from a digest of the RR and the id.

35. The medium of claim 34 wherein the code-ID is a hash of the RR concatenated with the id thereof.

36. The medium of claim 35 wherein the code-ID is a concatenation of two hashes, each hash being of the RR concatenated with the id thereof.